クレジットカードの個人情報流出に対するベンダーの責任

松本博

・はじめに

本稿は、東京地判平成二六年一月二三日（判例時報二二二一号七一頁）[1]の検討である。本判決は、ウェブサイトにおける商品の受注システムである「本件システム」を導入したユーザーに対する本件システムの設計・保守等を受託したベンダーの本件システムの構築についての債務不履行責任を認め、ベンダーに対して一億九一三万五五二八円及びこれに対する遅延損害金の支払を求めるユーザーの請求につき二二六二万三六九七円及びこれに対する遅延損害金の支払を求める限度で一部認容した第一審の裁判例である。

「システム開発契約」を巡っては、ユーザー（委託者ないし注文者）及びベンダー（受託者ないし請負人）の協力関係を前提に、同契約の締結時、履行時、さらに、履行後の各段階に応じて、ユーザーあるいはベンダーの債務不履行責任が問題となる場合が少なくない。

本件は、ウェブサイトにおける商品の受注システムの設計、製作、保守等の基本契約、個別契約が締結され、システムの完成後、ユーザーがシステムを稼動させていたが、顧客の個人情報、クレジットカード情報の流出が疑われる事態が発生し、ユーザーが原因調査、顧客対応等に伴うコストの負担を余儀なくされたため、ベンターに対する債務

不履行責任を追及した事案である。これまでに報道されているだけでも、本件のような顧客情報、信用情報の漏洩・流出事故・事件は現在までに多数発生しているが[2]、漏洩・流出の原因、情報の種類・内容、規模等の様々な事情によって、法的な責任の所在、内容も多様である。本件においては、流出の原因・規模等の調査、法的な責任の所在等が問題になったほか、契約上の責任制限の合意の成否、適用等も問題となった。

本判決は、ベンダーが受託契約上、契約当時の技術水準に沿ったセキュリティ対策を施したプログラムを提供することが黙示的に合意されていたことを認め、ユーザーに本件システムが導入ざれた後、本件システムを利用した顧客の情報が流出したことによって、「適切なセキュリティ対策が採られたアプリケーションを提供すべき債務の不履行」があったとして、ベンダーの債務不履行責任を肯定している。

［事実関係］

本件の事実関係は複雑であるが、判旨に関わる主要な部分は、概略以下の通りである。

・本件システムの導入までの経緯

X社（インテリア商材の卸小売、通信販売等を行う株式会社）は、Y社（情報処理システムの企画、保守受託及び顧客へのサポート業務、ホームページの制作、業務システムの開発、ネットショップの運営等を行う株式会社）との間で、平成二一年一月三〇日に、X社を委託者、Y社を受託者とする業務委託に係る「本件基本契約」及び覚書を締結した上で、同年二月四日、Y社に対し、注文書を交付して、X社のウェブサイトである「本件ウェブサイト」における商品の受注システムである「本件システム」の導入を合計八八九万五六〇〇円（消費税込み）で発注した。

・本件システムの導入とその利用状況

Y社は、X社用にカスタマイズした「本件ウェブアプリケーション」を製作して、本件システムを完成させ、平成二一年四月頃、X社による本件システムの検収を受けた。

X社は、平成二一年四月一五日、本件ウェブサイトの稼働を開始した。なお、この時点では、本件ウェブサイトを利用して商品を注文した顧客がクレジットカードを利用して本件ウェブサイトで商品を注文する際には、顧客はカード会社が管理するウェブサイトの画面上でクレジットカード情報を入力するため、本件サーバー内の「本件データベース」に顧客のクレジットカード情報は送信されていなかった。

本件システムの利用（保守サービス及びサーバーの利用）につき、X社は、平成二一年四月末頃、Y社に初年度利用料を支払った後、その後、その利用を一年ずつ更新して、最後の更新では本件システムの利用期間が平成二三年二月から平成二四年一月までとされていた。なお、この間、Y社は、A社との間でサーバー利用契約を締結し、A社が設置したレンタルサーバーである「本件サーバー」に本件システムのデータを保存していた。

・本件システムによる情報保存と流出

X社は、平成二二年一月頃、Y社に対し、本件ウェブサイトにおいて顧客が利用した決済方法（金種）について、従前はクレジットカード決済、代金引換又は銀行振込みの区別しかX社では把握できていなかったため、X社の基幹システム側で請求元情報を正確に管理する目的から、各種クレジットカード種別（カード会社）をX社の基幹システムに送信する旨の本件システムの仕様変更として「金種指定詳細化」を依頼し、同月二六日、そのための機能カスタマイズを発注した。

Y社は、同月二九日までに、金種指定詳細化を導入した本件システムについてX社による検収を受け、同日に金種指定詳細化を導入した本件システムを稼働させた。

その結果、同日以降は、顧客が本件ウェブサイトでクレジットカード決済を行う場合、本件サーバーにクレジットカード情報が入力され、その後本件サーバーとカード会社との間でクレジットカード情報のやり取りが行われるようになり、顧客のクレジットカード情報が暗号化されずに本件データベースに保存される設定となっていた。

X社とY社は、平成二二年五月一日、ウェブサイトのメンテナンスに係る「本件ウェブサイトメンテナンス契約」を締結した。

その後、平成二三年四月、本件サーバーに外部から不正アクセスがあり、顧客のクレジットカード情報を含む個人情報が流出することとなった。

［判旨］

本件でXの主張するYの債務不履行責任は、その一として、適切なセキュリティ対策が採られたアプリケーションを提供すべき債務の不履行、その二として、ネットワークやサーバーのセキュリティ対策を講ずべき債務の不履行、その三として、カード情報を保存せず、保存する場合には暗号化すべき債務の不履行、その四として、サーバー、データベース及び管理機能へのログインID及びパスワードを管理すべき債務の不履行、その五として、Yによるセキュリティ対策の程度についての説明義務違反からなる。

本判決は、①X社とY社との間での契約の概要、②本件システム等の概要、③金種指定詳細化に関する経緯、④本件流出発覚の経緯、⑤本件流出の原因及び被害範囲の特定について調査をしたB社の作成した調査報告書、⑥同じく本件流出の原因、被害範囲及び本件流出に関連する証拠データ等の特定について調査をしたC社の作成した調査報告書、⑦本件流出後の本件ウェブサイトの状況に係る認定事実を踏まえ、本件流出の原因がSQLインジェクション[3]にあることを前提に、この点に関係するYの債務不履行一、三及び五の責任につき、以下のとおり判示して、債務不履行一の責任を認め、債務不履行三及び五の責任を否定している。

・XとYとの間の契約関係

「Yが負うべき債務の内容を判断する前提として、XとYとの間の契約関係について検討すると、」「Yは、Xとの間で、本件基本契約を締結した上で、個別契約として、本件システムの製作（本件システム発注契約）、保守サービス（一年ごとに更新）、クレジットカード情報の把握（金種指定詳細化）、本件ウェブサイトのデザイン変更作業（本件ウェブサイトメンテナンス契約）等に係る本件個別契約を締結したのであるから、個別契約ごとに、当該個別契約及び本件基本契約に基づく債務を負うものと認められる（本件基本契約二条により、個別契約には本件基本契約が適用される。）」

これに対し、「Xは、Yとの間で締結した本件基本契約（同日に締結した覚書を含む。）、本件ウェブサイトメンテナンス契約及び本件基本契約に基づく各個別契約は全て一体の契約としてみるべきであると主張するが、本件基本契約及び本件個別契約は別の時期に締結されたものであり、個別契約ごとに内容も異なるのであるから、これらの契約を全て一体の契約としてみて、本件個別契約に基づき発生する債務を一体として把握することはできない」として、

Xの主張を認めなかった。

・債務不履行一（適切なセキュリティ対策が採られたアプリケーションを提供すべき債務の不履行）の責任

この点については、「Yは、平成二一年二月四日に本件システム発注契約を締結して本件システムの発注を受けたのであるから、その当時の技術水準に沿ったセキュリティ対策を施したプログラムを提供することが黙示的に合意されていたと認められる。そして、本件システムでは、金種指定詳細化以前にも、顧客の個人情報を本件データベースに保存する設定となっていたことからすれば、Yは、当該個人情報の漏洩を防ぐために必要なセキュリティ対策を施したプログラムを提供すべき債務を負っていたと解すべきである。」とし、その上で、「経済産業省は、平成一八年二月二〇日、「個人情報保護法に基づく個人データの安全管理措置の徹底に係る注意喚起」と題する文書において、ＳＱＬインジェクション攻撃によってデータベース内の大量の個人データが流出する事案が相次いで発生していることから、独立行政法人情報処理推進機構（以下「ＩＰＡ」という。）が紹介するＳＱＬインジェクション対策の措置を重点的に実施することを求める旨の注意喚起をしていたこと、ＩＰＡは、平成一九年四月、「大企業・中堅企業の情報システムのセキュリティ対策～脅威と対策」と題する文書において、ウェブアプリケーションに対する代表的な攻撃手法としてＳＱＬインジェクション攻撃を挙げ、ＳＱＬ文の組み立てにバインド機構を使用し、又はＳＱＬ文を構成する全ての変数に対しエスケープ処理を行うこと等により、ＳＱＬインジェクション対策をすることが必要である旨を明示していたことが認められ、これらの事実に照らすと、Yは、平成二一年二月四日の本件システム発注契約締結時点において、本件データベースから顧客の個人情報が漏洩することを防止するために、ＳＱＬインジェクション対策として、バインド機構の使用又はエスケープ処理を施したプログラムを提供すべき債務を負っていたということ

ができる。」

「そうすると、本件ウェブアプリケーションにおいて、バインド機構の使用及びエスケープ処理のいずれも行われていなかった部分があるから、Yは上記債務を履行しなかったのであり、債務不履行一の責任を負うと認められる。」

「Yは、Xが本件流出後に調査を依頼した大手調査会社であるラックですら、本件データベースへの侵入経路及び侵入手法は解明できていないから、本件流出は、専門業者の技術レベルを超える想定不可能な方法によって行われたものであり、Yにはその侵入行為について予見可能性がなかったと主張する。」

「しかしながら、Yが本件システム発注契約を締結した平成二一年二月四日時点で、SQLインジェクション攻撃によってデータベース内の大量の個人データが流出する事案が相次いで発生していること、SQLインジェクション対策として、SQL文の組み立てにバインド機構を使用し、又はSQL文を構成する全ての変数に対しエスケープ処理を行うことが必要であることが広く指摘されていたのであって、SQLインジェクション対策を講じていなければ、第三者がSQLインジェクション攻撃を行うことにより本件データベースから個人情報が流出し得ることはYにおいて具体的に予見可能であったということができ、それを超えて、個別の侵入態様を予見できなかったとしても、債務不履行一に係るYの予見可能性が否定されるものではない。したがって、予見可能性がなかったために過失がない旨のYの上記主張は理由がない。」

として、Yの反論を排斥して、Xの主張するYの債務不履行一の責任を認めている。

・債務不履行三（カード情報を保存せず、保存する場合には暗号化すべき債務の不履行）の責任

この点については、「厚生労働省及び経済産業省が平成一九年三月三〇日に改正した「個人情報の保護に関する法

律についての経済産業分野を対象とするガイドライン」（同日厚生労働省・経済産業省告示第一号）では、クレジットカード情報等（クレジットカード情報を含む個人情報）について特に講じることが望ましい安全管理措置として、利用目的の達成に必要最小限の範囲の保存期間を設定し、保存場所を限定し、保存期間経過後適切かつ速やかに破棄することを例示し、ＩＰＡは、同年四月、「大企業・中堅企業の情報システムのセキュリティ対策～脅威と対策」と題する文書において、データベース内に格納されている重要なデータや個人情報については暗号化することが望ましいと明示していたことが認められる。しかし、上記告示等は、いずれも上記対策を講じることが「望ましい」と指摘するものにすぎないし、上記ＩＰＡの文書においては、データベース内のデータ全てに対して暗号化の処理を行うとサーバー自体の負荷になることがあるので、特定のカラムだけを暗号化するなどの考慮が必要であるとも指摘されているように、暗号化の設定内容等は暗号化の程度によって異なり、それによってＹの作業量や代金も増減すると考えられることに照らすと、契約で特別に合意していなくとも、当然に、Ｙがクレジットカード情報を本件サーバー及びログに保存せず、若しくは保存しても削除する設定とし、又はクレジットカード情報を暗号化して保存すべき債務を負っていたとは認められない。」

として、Ｙには債務不履行三の責任を否定した。

・債務不履行五（Ｙによるセキュリティ対策の程度についての説明義務違反）の責任

この点については、「Ｘは、システム設計、開発及び運用を行う業者であるＹは、発注者であるＸに対し、Ｘが本件システムのセキュリティ対策の程度及び情報流出の危険性を認識し、セキュリティ対策について選択できるように説明すべき信義則上の義務を負うと主張し、Ｙが説明すべき具体的内容としては、〈一〉ＳＱＬインジェクション対

策を講じていないこと、〈二〉本件システムのセキュリティ対策が脆弱であること、〈三〉Yとさくらインターネット株式会社との間のレンタルサーバー契約において最低のセキュリティレベルの内容としていたこと、〈四〉金種指定詳細化の際に、クレジットカード情報を暗号化せずに保存する設定としたことを指摘する。」

しかし、「〈一〉については、YがSQLインジェクション対策を講じていないことは、XとYとの間での本件システム発注契約に基づき発生する、個人情報の漏洩を防ぐために必要なセキュリティ対策を施したプログラムを提供すべき債務の不履行（債務不履行一）に当たるのであるから、それとは別に、信義則上の義務として、YがSQLインジェクション対策を講じていないことを説明すべき義務を負うとは認められない。」

「〈二〉については、本件流出の原因はSQLインジェクションと認められる一方、その他の本件システムのセキュリティ対策が脆弱であることが本件流出に寄与したことを認めるに足りる証拠はないから、Yが本件システムのセキュリティ対策が脆弱であることを説明すべき義務を負うとは認められない。」

「〈三〉については、Yとさくらインターネット株式会社との間のレンタルサーバー契約において最低のセキュリティレベルの内容としていたことを裏付ける証拠はないから、かかる事実は認められず、かかる事実を説明すべき義務を負うとするXの主張は前提を欠くために採用できない。」

「〈四〉については、Xのシステム担当者は、Yの取締役からの回答により、現状はデータベースにクレジットカード情報のデータはあるが、データベースを直接見る手法を用いなければカード番号は見られないこと、セキュリティ上はクレジットカード情報を保持しない方が良く、その方が一般的であることを認識していたことが認められ、Yはクレジットカード情報の保存による危険性を説明したといえるから、Yにはクレジットカード情報を暗号化せずに保存する設定としたことについての説明義務違反は認められない。」

として、Ｙの債務不履行五の責任を否定した。

・本件基本契約二九条二項の適用の有無

本件基本契約二九条二項は、一定の合理性があるとして、「本件基本契約二九条二項は、Ｙに故意又は重過失がある場合には適用されないと解するのが相当である。」としたうえで、Ｙに重過失が認められるかにつき、Ｘの挙げたＹの重過失の評価根拠事実のうち、〈一〉の電子商取引システムの設計・構築に当たってＳＱＬインジェクション攻撃への対策を講じることは専門業者として当然であったこと、について検討し、「Ｙは、情報処理システムの企画、ホームページの制作、業務システムの開発等を行う会社として、プログラムに関する専門的知見を活用した事業を展開し、その事業の一環として本件ウェブアプリケーションを提供しており、Ｘもその専門的知見を信頼して本件システム発注契約を締結したと推認でき、Ｙに求められる注意義務の程度は比較的高度なものと認められるところ、前記のとおり、ＳＱＬインジェクション対策がされていなければ、第三者がＳＱＬインジェクション攻撃を行うことで本件データベースから個人情報が流出する事態が生じ得ることはＹにおいて予見が可能であり、かつ、経済産業省及びＩＰＡが、ウェブアプリケーションに対する代表的な攻撃手法としてＳＱＬインジェクション攻撃を挙げ、バインド機構の使用又はＳＱＬ文を構成する全ての変数に対するエスケープ処理を行うこと等のＳＱＬインジェクション対策をするように注意喚起していたことからすれば、その事態が生じ得ることを予見することは容易であったといえる。また、バインド機構の使用又はエスケープ処理を行うことで、本件流出という結果が回避できたところ、本件ウェブアプリケーションの全体にバインド機構の使用又はエスケープ処理を行うことに多大な労力や費用がかかることをうかがわせる証拠はなく、本件流出という結果を回避することは容易であったといえる。」として、Ｙの重過失を認めた。

・Xの過失について

なお、X側の過失については、「Yからは過失相殺の主張はないが、」「Xのシステム担当者が、顧客のクレジットカード情報のデータがデータベースにあり、セキュリティ上はクレジットカード情報を保持しない方が良いことを認識し、Yから本件システム改修の提案を受けていながら、何ら対策を講じずにこれを放置したことは、本件流出によるクレジットカード情報の漏洩の一因となったことは明らかであるから、Xに損害が認められるとしても、上記Xの過失を考慮し、三割の過失相殺をするのが相当である（上記の過失相殺事由は、因果関係の断絶を基礎付ける事実として当事者が十分な攻撃防御をしているから、過失相殺をすることは弁論主義に反せず、当事者への不意打ちともならない。）。」としている。

（なお、上記判決文中の網掛けおよび下線は筆者によるものである。）

［先例・学説］

本件は、「システム開発契約」をめぐって、ベンダーの債務不履行責任が問題となっている事案である。同旨の問題に関する先例として、東京地判平二四・三・二九判タ一四〇五号二五四頁、その控訴審判決である東京高判平二五・九・二六金判一四二八号一六頁のほか、東京地判平二五・一一・一二判タ一四〇六号三三四頁、東京地判平二六・一一・五金判一四六〇号四四頁がある。

また、学説をみると、前掲東京地判平二四・三・二九及び前掲東京高判平二五・九・二六の判例評釈等である、河上正二・金法二〇〇一号七一頁、桶田大介・ＮＢＬ一〇一三号四頁、滝澤孝臣・銀行の業務全般をつかさどる経営シ

ステムの開発契約につきベンダの「プロジェクト・マネージメント義務」違反を理由とするユーザの契約解除が認められた事例」私法判例リマークス四七号一八頁がある。

ベンダーの債務不履行責任が認められるか否かは、事実関係の判断として位置付けられる問題といえる。債務不履行責任を認めること自体については、先例であっても、学説であっても、特に異論はみられない。

［検討］

本事案において裁判所の下した結論自体は支持できるものである。しかし、個別の論点についての判断には承服しがたい点もある。以下検討を進める。

・ベンダーとユーザー

ベンダー（vendor）とは、売る人、売り手、売り主、販売者、販売店などの意味を持ち、製品やサービスを利用者に販売する事業者のことを意味する。販売する製品の種類や分野を冠して「ハードウェアベンダー」「ＯＳベンダー」「システムベンダー」といった形で「〇〇ベンダー」というように造語を構成しているようである。

ベンダーは、製品やサービスを買い手・利用者に対して販売する者のことを指し、自らがその製品を開発・製造しているとは限らない。製造元あるいは販売元のことは「メーカー」（maker）、買い手・利用者のことは「ユーザー」（user）あるいは「エンドユーザー」（end user）という。ベンダーは、企業などに対し複数の機器やパッケージソフトなどを組み合わせて情報システムを開発・納品するような事業（SI: System Integration システムインテグレー

ションと呼ばれる）では、システムの開発・販売元を「システムインテグレーター」（System Integrator）あるいは単に「インテグレーター」（integrator）といい、システムに含まれる機器やパッケージソフトの販売者（購入先）のことをベンダーということがある。

一方で、情報システムの買い手・利用者の側（ユーザー企業）からは、インテグレーターのことをシステム全体の売り主として「ＩＴベンダー」「システムベンダー」「開発ベンダー」などということがある。システムインテグレーターとは、顧客の業務内容を分析し、問題に合わせた情報システムの企画、構築、運用などの業務を一括して請け負う業者のことである。システムの企画・立案からプログラムの開発、必要なハードウェア・ソフトウェアの選定・導入、完成したシステムの保守・管理までを総合的に行う。このような事業のことをシステムインテグレーション（SI: System Integration）という。

ベンダーという言葉には製造販売という意味合いが含まれている。システムインテグレーターは主に他社製品を使用して企画から運用までの業務を請け負うのに対して、ベンダーは自社製品と製品を組み合わせてシステム構築し、その中に自社製品の販売が含まれている点で厳密には両者は異なっている。

この点において、ベンダーという言葉の使用や解釈には留意する必要がある。

・システム開発契約をめぐる債務不履行責任

システム開発契約につき、ベンダーのユーザーに対する損害賠償責任の有無をめぐって争われている事案のうち、ベンダーに責任が認められている先例として、広島地判平一一・一〇・二七判時一六九九号一〇一頁、東京地判平二・三・三〇判時一三七二号一〇一頁などが、反対に、ユーザーに責任が認められている先例として、東京地八王

子支判平一五・一一・五判時二八五七号七三頁、東京地判平九・九・二四判タ九六七号一六八頁、前掲東京地判平二・三・三〇などがある。東京地判平一六・三・一〇判タ一二一一号一二九頁[4]では、システム開発契約におけるベンダーのプロジェクト・マネジメント義務と、ユーザーの協力義務とを認めた上で、ベンダーの責任も、ユーザーの責任も否定している。ベンダーと、ユーザーとが、形式的には、対内的な当事者として捉えざるを得ないとしても、システム開発に向けた共同的な当事者として捉え、その相互関係の下に、ベンダーの義務と、ユーザーの義務とを合目的的に関連づけ、システム開発が頓挫した場合の責任の所在を検討している。X（注文者）とY（請負人）との間で、システムの開発を目的とした請負契約が締結されたという事案であるが、同判決は、一方で、「Yは、システム開発の専門業者として、自己が有する高度の専門的知識と経験に基づき、本件電算システム開発契約の契約書及び本件電算システム提案書において指示した開発手順や開発手法、作業工程等に従って開発作業を進めるとともに、常に進捗状況を管理し、開発作業を阻害する要因の発見に努め、これに適切に対処すべき義務を負うものと解すべきである」から、「注文者であるXのシステム開発へのかかわりについても、適切に管理し、システム開発について専門的知識を有しないXによって開発作業を阻害する行為がされることのないようXに働きかける義務（プロジェクトマネージメント義務）を負っていた」とし、他方で、「本件電算システムの開発は、Xと受託者であるYの共同作業というべき側面を有する」ので、「Xは、契約書にも明記されているとおり、本件電算システムの開発過程において、資料等の提供その他本件電算システム開発のために必要な協力をYから求められた場合、これに応じて必要な協力を行うべき契約上の義務（協力義務）を負っていた」とした上で、当該事案では、当該システムが「納入期限までに完成に至らなかったのは、いずれか一方の当事者のみの責めに帰すべき事由によるものというのは適切ではなく、XとY双方の不完全な履行、健保法改正その他に関する開発内容の追加、変更等が相まって生じた結果であり、いずれか一方の

当事者が債務不履行責任を負うものではな」いと判示している。

学説は、プロジェクト・マネジメント義務と、協力義務とを認めた上で、その相関関係に立つ履行の必要性を前提に、いずれかの責任を肯定し、反対に、いずれの責任も否定、あるいは、肯定するといった先例にみられる判断枠組を承認する見解が一般的である。[5]

・本件について

本件システム発注契約における債務不履行責任

以上の見地から本件システム発注契約についてみると、本件システムが完成してこれをユーザーが導入した後に、本件システムのサーバー上に保存されていた顧客のデータが流出したというのが「本件流出」であるが、本判決の認定によれば、本件流出の原因はＳＱＬインジェクションにあるというのであって、その対策としては、バインド機構の使用及びエスケープ処理があるにもかかわらず、Ｙは、その対策を講じていなかったというのであるから、本件システムを利用した顧客の情報の流出を防止しなければならないことを経済産業省の注意喚起の事実を踏まえて当然の前提とすれば、この点において、Ｙの「適切なセキュリティ対策が採られたアプリケーションを提供すべき」債務不履行一の責任は免れない事案であると解される。

本件システムは、当初、顧客の情報がシステム内に保存される仕組みではなかったものの、後にＸの要望に従って、本件システムに金種指定詳細化を導入したことに伴い、顧客の情報がシステム内に保存されるようになった。この場合、システムに保存された顧客の情報が流出しても差し支えないとの意向で、Ｘが金種指定詳細化の導入をＹに求めたとは考えられないことから、この点も、Ｙの責任を否定することにはならないはずである。

これに対し、裁判所は、Ｙの「カード情報を保存せず、保存する場合には暗号化すべき」債務不履行三の責任、Ｙによる「セキュリティ対策の程度についての説明義務」についての債務不履行五の責任をいずれも否定している。裁判所の見解としては、Ｙの「カード情報を保存せず、保存する場合には暗号化すべき」債務不履行三の責任については、暗号化につき契約で特別に合意しているわけではないのだから、顧客の情報の暗号化をベンダーに義務付けることはできないと解しているのでありＹによる「セキュリティ対策の程度についての説明義務」についての債務不履行五の責任については、顧客の情報を暗号化しないで保存したことのベンダーの説明義務ないし同義務違反は認められないというのである。

システム開発契約をめぐる債務不履行責任が問題となる場合には、システムの開発がユーザーとベンダーの協力関係を前提に成り立つものであるため、ベンターの債務不履行責任として「プロジェクト・マネジメント義務」及びその違反の有無・程度が検討されるだけでなく、併せて、ユーザーの債務不履行責任としていわゆる「協力義務」及びその違反の有無・程度も検討されるのが一般的である。

本件システムに保存された顧客の情報が不正なアクセスによって流出することを防ぐ方策自体について、ユーザーの協力といったものは観念し難いが、その流出ないし流出後の利用を防止する方策として情報の暗号化が考えられるとしても、ユーザーの指示といった協力関係がないのに、ベンダーがその暗号化を義務付けられるものとは観念し難いものであるとして、この点に関する本判決の判断は、契約解釈の問題として、是認されるべきものとして肯定的にとらえる見解もある。[6]

裁判所は、厚生労働省・経済産業省のガイドラインで安全管理措置として、利用目的の達成に必要最小限の範囲の保存期間を設定し、保存場所を限定し、保存期間経過後適切かつ速やかに破棄することの例示やＩＰＡの文書によっ

て、データベース内に格納されている重要なデータや個人情報については暗号化することが望ましいと明示していたことを認めている。しかし、これはいずれも上記対策を講じることが「望ましい」と指摘するものにすぎないし、ＩＰＡの文書においては、データベース内のデータ全てに対して暗号化の処理を行うとサーバー自体の負荷になることがあるので、特定のカラムだけを暗号化するなどの考慮が必要であるとも指摘されているように、暗号化の設定内容等は暗号化の程度によって異なり、それによってＹの作業量や代金も増減すると考えられることに照らすと、契約で特別に合意していなくとも、当然に、Ｙがクレジットカード情報を本件サーバー及びログに保存せず、若しくは保存しても削除する設定とし、又はクレジットカード情報を暗号化して保存すべき債務を負っていたとは認められない、とする。

しかしながら、現代社会において個人情報、それもクレジットカードという極めて重要な個人情報にかかる安全管理措置について対策を講じることを「望ましい」レベルで捉えてもよいのだろうか。システム開発・管理の専門家であれば管理の一環としてデータベース内に存在するデータや個人情報については当然に暗号化するといった配慮が求められるべきである。

本件システム契約の当事者の属性をみると、いずれも商人（株式会社）である。その点では、Ｂ to Ｂ取引の外形を呈している。しかし、Ｘはインテリア商材の販売等を業とする者であり、Ｙは業務システムの販売等を業とする者である。ＸはシステムＹに通じていないからこそ、本件ではシステムの専門家であるＹに業務を委託したものと考えるのが妥当であろう。そもそもＸにシステムについての十分な知識・経験があったのであれば、自らシステムを管理することも可能であり（Ｙにしても無償配布ソフトであるＥＣ－ＣＵＢＥをベースとして構築していた）、あるいはＸはパートナーとして対等にシステムの構築・維持に携わることもあり得たであろう。法的な意味ではイーブンな関係

にあるとしても、システム技術等に関する極めて専門的な内容についてはベンダーとユーザーは対等とは言い難いケースのほうが多いといえる。この場合には、素人とプロが契約当事者となるに等しい状況が生じているにも関わらず、そうした事情を全く考慮することなく当事者をイーブンに取り扱う契約がなされてしまうことには違和感を覚える。システム管理のプロフェッショナルとしてのYは原則として顧客のデータについての暗号化処理は当然に行うべきだったのではないだろうか。もちろん、これは原則としてということであり、裁判所も言及しているようにデータベース内のすべてのデータを暗号化することがサーバーに過大な負荷を与えてしまうケース等があるとすれば、その場合には、別途追加料金の支払いや契約の変更を生じせしめることはありえるだろう。

Xの過失

X側の過失につき、裁判所は、「Yからは過失相殺の主張はないが、」「Xのシステム担当者が、顧客のクレジットカード情報のデータがデータベースにあり、セキュリティ上はクレジットカード情報を保持しない方が良いことを認識し、Yから本件システム改修の提案を受けていながら、何ら対策を講じずにこれを放置したことは、本件流出によるクレジットカード情報の漏洩の一因となったことは明らかであるから、Xに損害が認められるとしても、上記Xの過失を考慮し、三割の過失相殺をするのが相当である。」としている。

しかし、前述の通りシステム管理のプロフェッショナルとしてのYは原則として顧客のデータについての暗号化処理は当然に行うべきだった。この点で本件におけるY側の基本的な責任は否めない。

ただし、裁判所の認定によると、Xにはシステム担当者が存在していたようである。その時々のセキュリティに関する情報を適切に把握した上で、自己の財務状況等諸般の事情を勘案した対策を講じることがいずれの企業において

もシステム担当者一般に課された責務であろう。インテリア商材の販売等を業とするXの担当者にYと同様のシステムの技術上のスキルは求めるべくもない。けれども、少なくとも当時の状況にあってXとしてはどの程度のセキュリティ対策を採用することが望ましいのかについての状況把握は、Xのシステム担当者として当然に求められることである。それにもかかわらず、当時の一般論としてのセキュリティレベル、Yからの提案等を踏まえた考慮をなすべき立場にあったXのシステム担当者が何らの対策を講じずに放置したことは、X側には看過できない過失があったとの判断が下されても致し方のないことである。したがって、この点における裁判所の判断は妥当なものといえる。

・本判決の意義

以上のとおり、本判決は、ウェブサイトにおける商品の受注システムを利用した顧客の情報が流出した場合に、同システムの設計・保守等を受託していたベンダーのシステムの構築についての債務不履行責任（適切なセキュリティ対策が採られたアプリケーションを提供すべき債務の不履行）を認めた裁判例である。

システム開発契約をめぐる当事者（ベンダーおよびユーザー）の法的紛争の解決に当たっては、必ずしもその中核が事実問題にとどまるわけではなく、当然法律問題としての検討が中心となる場合もある。しかし、本件で問題となっているシステムに保存された顧客情報の流出防止といった観点からすると、これについては専ら事実問題として解決し得る場合であるものと解される。ベンダーの債務不履行責任を認めた本判決の結論については異論はないものの、その判断のファクターとしてベンダーとユーザーの背景（属性）を考慮せずに結論を下した点については疑念が残る。本検討では、事実関係と、これを前提とした本判決の認定判断に重きを置いたが、システム開発契約を巡る法的紛争を検討することは今後の展開を想定しても更に重要性を増すものと考える。

注

・本稿の表記について―語尾「ー」の取り扱い

本稿においては、「コンピューター」と「コンピュータ」、「ユーザー」と「ユーザ」、「ベンター」と「ベンダ」といった語尾に「ー」の表記があるものとないものが入り乱れている。

たとえば、「コンピューター」については、一般的に、マスメディアでは「コンピューター」と表記することが多いようである。これは、外来語の表記について昭和二九年に国語審議会から、「原語（特に英語）のつづりの終わりの -er、-or、-ar などをかな書きにする場合には、長音記号『ー』を用いる」と発表されたことによる。その後、国語審議会の報告を基に告示された一九九一年の内閣告示第二号では、英語由来のカタカナ用語において、言語の末尾が -er、-or、-ar などで終わる場合に長音表記を付けることが推奨されている。

一方で、科学専門の雑誌等で見かけるのが「コンピュータ」という表記である。これは電気関係など一部の専門分野で以前から使用されていた専門表記で、後に文部科学省の『学術用語集』にも「コンピュータ」と記載されるようになったという背景がある。理系の学問や技術関係の出版物に「コンピュータ」と表記されているのはこのことによるものと思われる。いずれが正しいと断言できる性質のものではないが、筆者としては「コンピューター」の表記を用いることとしている。なお、原典において「コンピュータ」という表記が用いられているものについてはそのままの表記としている。

1　本件評釈として、滝澤孝臣　ウェブサイトにおける商品の受注システムを利用した顧客の情報が流出した場合に同システムを導入したユーザに対する同ユーザから同システムの設計・保守等を受託していたベンダの同システムの構築に係る債務不履行責任が認められた事例　私法判例リマークス五一号三〇頁　二〇一五年、浅井弘章　顧客のクレジットカード情報が流出した事故についてベンダーの債務不履行責任が認められた事例〈金融商事実務判例紹介〉銀行法務二一　七八四巻一一五頁　二〇一四年九月、上山浩　ソフトウェアのセキュリティ対策の脆弱性により情報流出が生じた事件の判決の実務的検討ＮＢＬ一〇五五号三四頁　二〇一五年八月、遠藤元一　ウェブサイトによる商品の受注システムを利用した顧客のクレジットカード情報が流出した事故につき、システムの設計、製作、保守等の受託業者の債務不履行に基づく謝罪・問合わせ等の顧客対応費用、売上損失等の損害賠償責任が肯定された事例　横浜法学二四巻二・三号一九一頁　二〇一六年三月

2　アメリカのYahoo!は、二〇一六年九月二二日、同社サービスの利用者五億人超の個人情報が流出していたことを発表した。流出したのは名前および電話番号、生年月日、メールアドレス、暗号化されたパスワード、本人確認のために利用者が設定した質問と答えなどであり、銀行口座やクレジットカードなどについては流出していないという。

五億件以上の個人情報流出というのは最大規模で、政府の支援を受けたサイバー攻撃の可能性もあるという。また、いつ流出が確認されたかは明らかにされていない。ユーザーらがYahoo!に対し、顧客データの保護を怠ったとして提訴する動きも相次いでいるようである。（二〇一六年九月二三日　読売新聞、朝日新聞、TechCrunch）

検索サイト「Yahoo! Japan」を運営している日本のYahoo!は、アメリカのYahoo!とは異なるシステムを使っており、日本でのサービスのほとんどは独自に運営されているため、現時点では「情報流出の被害は確認されていない」としている。

二〇一六年六月には、旅行会社大手ＪＴＢは、グループ会社に不正アクセスがあり、七九三万人分もの個人情報が流出した可能性があると発表したが、様々なところでWeb上での個人情報の漏洩事件が多発している。

3　本件で問題となるＳＱＬ（Structured Query Language）とは、データベースの管理プログラムを制御するためのコンピュータ言語をいい、一件のデータを複数の属性の値の組として表現し、組を列挙することでデータを格納していく方式である。ＳＱＬインジェクションまたはＳＱＬインジェクション攻撃（(SQL injection)）とは、データベースと連動したウェブサイトで、データベースへの問い合わせや操作を行うプログラムにパラメータ（IT の分野では、ソフトウェアやシステムの挙動に影響を与える、外部から投入されるデータなどのことをいう）としてＳＱＬ文（データベースへのテーブルの追加や設定変更、削除、テーブル間の関係の定義や削除、テーブルへのデータの追加、更新、削除、データベースやシステムの設定変更などを行うための命令語と構文、文法）の断片を与えることにより、データベースを改ざんしたり不正に情報を入手したりすること、あるいは、そのような攻撃を許してしまうプログラムの脆弱性のことをいう。ＳＱＬインジェクションはパラメータをＳＱＬ文に埋め込む際にきちんとチェックが行われていないために起こる。

ＳＱＬインジェクションの脆弱性対策としては、バインド機構とエスケープ処理がある。バインド機構とは、あらかじめＳＱＬ文のひな型を用意し、後から変動個所（プレースホルダ）に実際の値（バインド値）を割り当ててＳＱＬ文を生成するデータベースの機能である。ＳＱＬ文のひな型とバインド値は個別にデータベースに送られ、構文解析されるので、バインド値に悪意あるＳＱＬ文が挿入されても、その実行を阻止することができる。

ＳＱＬステートメントを書く時に必ずバインド機構を使用すれば、バインド機構に不具合がない限り、ＳＱＬインジェクションは不可能だと考えられる。

エスケープ処理とは、ＳＱＬインジェクションのために挿入された文字列を攻撃が成功しないように文字列の置き換えを行う処理を指す。例えば、「'」を「''」に変換し、「\」を「\\」に変換するなどの処理である。

ＳＱＬ文を入力直後にエスケープ処理を行うと、ＳＱＬ文を生成する直前に別の文字列操作が行われた場合、ＳＱＬインジェクションが成功する文字列が完成してしまう可能性があるため、エスケープ処理は、生成する直前に実施することになる。

4　本判決の判例評釈等として、小林秀之「金融システム開発契約に係る法的諸論点の帰趨」金法一九五二号五二頁、同「金融機関のシステム開発と法的問題」銀法七四五号八頁、樋田大介「情報システム開発契約の多段階契約に関する新しいアプローチの必要性」ＮＢＬ九七七号四頁などがあるほか、前掲東京地判平一六・三・一〇の判例評釈等（前同）として、生田植康「電算システム開発契約における注文者の協力義務と請負人のプロジェクトマネージメント義務」福法五二巻四号四七一頁、高田寛「システム開発における請負人のプロジェクトマネジメント義務および損害賠償をめぐる争い」ＮＢＬ九九〇号一二一頁などがある。

5　個別的な論証として、吉田析代「システム開発契約における典型契約の意義と債務内容の事後的判断基準―情報システム・モデル取引・契約書における役割分担を題材に」新報一一四巻一一＝一二号七五一頁、元吉芳郎「共同開発契約―成果の帰属と利用を中心に」判タ一三七五号二五頁、清水建成「システム開発契約における紛争―契約成立と仕様変更に伴う問題」判タ一三三五号二四頁、コンピュータ訴訟研究会『コンピュータ紛争事件のケース研究』、同『コンピューター紛争Ⅱ』がある。また、ソフトウェア開発関係訴訟を対象として、その訴訟実務の在り方・進め方を分析したものとして、東京地方裁判所プラクティス委員会第二小委員会編「ソフトウェア開発関係訴訟の手引き」判タ一三四九号四頁、田中俊次＝山田陽三ほか「ソフトウェア開発関係訴訟の審理」判タ一三四〇号四頁があるほか、裁判例を概観して問題点を整理したものとして、滝滞孝臣「システム開発契約の裁判実務からみた問題点」判タ一三一七号五頁（現代企業法研究会編著『企業間提携契約の理論と実務』所収）がある。

6　滝澤孝臣 ウェブサイトにおける商品の受注システムを利用した顧客の情報が流出した場合に同システムを導入したユーザに対する同ユーザから同システムの設計・保守等を受託していたベンダの同システムの構築に係る債務不履行責任が認められた事例私法判例リマークス五一号三三頁 二〇一五年